

## MANAGING ACCESS TO PHYSICAL ASSETS

### Related Applications

This application is a continuation-in-part of Application No. 10/356,655, filed  
5 January 31, 2003, and a continuation-in-part of Application No. 10/356,383, also filed  
January 31, 2003. This application is also a continuation-in-part of Application  
No. 10/363,938, filed March 6, 2003, which is a § 371 U.S. National Stage of International  
Application No. PCT/US02/13653, filed April 30, 2002. Each of these prior applications is  
incorporated herein by this reference.

10

### Field

This application relates to asset management and tracking, and more specifically, to  
managing and tracking physical assets, such as, e.g., keys or other objects, that are secured at  
remote locations but must be accessed and used by different authorized people for various  
15 purposes.

15

### Background

Asset management systems, such as key management systems, are known. Effective  
key management requires that a number of individual keys can be securely stored when not  
20 in use, but one or more of the keys can be made available to an authorized user in an  
efficient manner. Enhanced capabilities of key management systems would include tracking  
of keys that are in use or missing, as well as the ability to generate reports about activity  
relating to access of the keys and/or the locked areas unlocked by the keys.

20

In one type of application, key management systems are used to administer the use of  
25 keys for a large fleet of vehicles, e.g., at a car dealership. The dealership expects the system  
to assist in permitting only authorized individuals, e.g., salespersons, mechanics, managers,  
etc., to have access to vehicles in its possession, but it does not wish to impede these  
authorized individuals from conducting business with cumbersome security measures.

25

According to one current approach, vehicle keys are maintained in a centralized  
30 location, e.g., the dealership showroom. In today's larger dealerships, returning from the

30

sales lot to the showroom each time a different key is needed may pose a real inconvenience. Therefore, a salesperson may try to guess all of the vehicles that a sales prospect may be interested in, and then take the keys to these vehicles. The keys may not be returned to the centralized location for some time, because the salesperson is busy or because the salesperson gives the keys to another salesperson who is seeking them. As a result, some keys may be "out of circulation" for an extended period, even though they may not be in actual use.

Some centralized systems are as simple as a key board having hooks on which the keys are hung, thus providing a visual indication of which vehicles are available on the lot based on which keys are present on the board. Another centralized system requires each individual seeking access to login through an attached computer with an ID and a password. Authorized individuals are provided access to a secure drawer with a compartment assigned to the keys for each vehicle in the dealership's inventory. This system records who removes a key from the drawer, the time the key was removed, and the time it was returned, based in part on an electronic identifier attached to each vehicle's keys. One problem with such centralized electronic systems, however, is that when they inevitably fail, the secured keys to an entire inventory of vehicles cannot be accessed until the problem is corrected.

According to another current approach, which is decentralized, the keys are securely stored at or near each parked vehicle. The keys to each vehicle (or at least the ignition key) are secured in a locked key container when not in use. For example, each vehicle can be outfitted with a key box or key container having a conventional lock accessed by a conventional key, such as the present assignee's Indigo® key box. A dealership's collection of key containers might be keyed alike, or might require a small number of different keys.

In any case, theft or loss of one of the keys to the key containers poses a security risk until detected. It is also expensive to retool each lock to accept only a new key that has not been compromised. There are also limits on the number of different new keys that can be made for conventional locks, so a careful thief with a collection of stolen keys still might have access.

There are also drawbacks to using the conventional key container in its intended way. A busy salesperson may forget to replace the keys in the key container for a first vehicle

before taking a sales prospect for a test drive in a second vehicle. There is a chance that the salesperson may eventually return both sets of keys, but may return them to the wrong key containers. There is no way to track past accesses with the conventional key container system.

5 Another type of decentralized system also makes use of remotely located key containers secured by conventional locks, but each user has a custom-cut conventional key capable of accessing each key container. This system is able to track which custom-cut key was used to access which key container, but there is no assurance that the current key user is the assigned user. Loss or theft of the custom-cut key requires all of the key containers to be  
10 re-keyed, which is expensive. The key container of this system communicates access information to a centralized location, but this requires a supply of power and associated circuitry that makes this container much more expensive.

It would be advantageous to provide a key management system that addresses some of the drawbacks of the prior systems.

15

### Summary

The asset management system and methods of this application provide advantages compared to prior art approaches.

First, the system and methods of this application can be used under a decentralized  
20 approach that allows the keys to be stored at secure locations near each respective vehicle, rather than requiring a user seeking access to first obtain the vehicle keys from a central location that may be far removed from the vehicle that the user seeks to access.

Second, the access device that allows an authorized user to access a key container in which the vehicle keys are secured is a portable electronic device that is preprogrammed  
25 with the user's privileges and periodically expires. In addition, the user must enter identifying information, such as a PIN code, to authenticate himself before access is allowed. Thus, loss or theft of an access device poses less risk than loss of a conventional key that may provide access to a large number of key containers.

According to one implementation, a key management system for controlling access  
30 to vehicle keys includes a key set, a key container and a portable electronic access device.

The key set includes vehicle keys to a particular vehicle and a key tag associated with the vehicle keys. The key tag has an electronically readable identifier stored on the key tag.

The key container can be located on or near the vehicle. The key container has a key set storage area secured by an electronic lock. The key container can detect the presence of the key tag within the key set storage area. For example, the key tag can have an electrical contact portion that completes a circuit in the key container when the key set is stored in the key set storage area.

The portable electronic access device is carried by a user to access the key container. The access device has a memory that is updated with at least the identifier of the key tag when the key container is successfully accessed and the key set is removed from the key set storage area.

The memory in the access device can also record the approximate time that a successful access was made. The memory of the access device can include stored privileges, and at least some of these privileges can be set to expire periodically.

The access device can be configured to supply the electrical power necessary to operate the circuit of the key container. The system can be configured to require that the user physically connect the access device to the key container to establish a communications link. In other implementations, the access device can establish a wireless communications link with the key container and does not supply power to the key container.

The access device can be programmed with access privileges corresponding to the user's identity. The key container is usually programmed to prevent access unless the user validates his identity.

The key container can include a memory that stores, e.g., the identifier of the key tag of the stored key set and/or an access log providing information identifying which users recently accessed the key container, which key tags were accessed and at what times. The memory of the key container can include a lockout list identifying an unauthorized access device or an unauthorized user.

The key container can include an attachment portion shaped to allow the key container to be supported over an edge of a window in the vehicle.

The system can include a central computer and an associated database for use in administration, include assigning privileges to different classes of users, updating information about current inventory to be tracked, tracking activity of access devices, users and vehicles, and allowing certain classes of users to generate and view reports of activity.

5 Users can log into the central computer to reestablish their expired access privileges.

Prior to or during an access event, the user demonstrates that he is authorized, which may include communicating identification information to the access device, e.g., entering a PIN code on a key pad or other similar authentication routine. Once initially authorized, the user may then be asked to select from one of a predetermined group of codes corresponding  
10 to the purpose of the access.

With an access device that is programmed to expire periodically, the information stored in the memory of an expired access device can be automatically uploaded to a database before reuse, e.g., at check in, during reauthorization, etc.

According to another implementation, a key management system for controlling  
15 access to a vehicle key stored proximal to a remotely located vehicle includes a key container, a key tag associated with the vehicle key and an electronic key for accessing the key container. The key container is located proximal to one of the remotely located vehicles. The key container has a key storage area for storing a vehicle key associated with the respective vehicle and is secured by an electronic lock. The key container has a memory that  
20 is capable of recording information when the key storage area is accessed. The key tag has an electronically stored identifier and is detectable by the key container when placed in the key storage area. The electronic key is capable of establishing a wireless communications link with the electronic lock of the key container and has a memory. Information about access events is stored in the key container memory and/or the memory of the electronic key.

25 The wireless communications link can be an infrared link. The electronic key can be an open architecture personal digital assistant or an open architecture mobile phone.

According to another implementation, a key management system for controlling access to vehicle keys includes a key set, a key container and an open architecture electronic access device. The key set includes a vehicle key to a particular vehicle and a key tag  
30 associated with the vehicle key. The key tag has an electronically readable identifier stored

on the tag and an electrical contact portion. The key container can be located on or near the vehicle. The key container has a key set storage area secured by an electronic lock. The key container is capable of detecting the key set when the key set is properly stored in the key set storage area. The electronic access device can be carried by a user to access the key  
5 container. The access device has a memory that is updated with at least the identifier of the key tag when the key container is successfully accessed and the key set is removed from the key set storage area.

The key container can include a memory that stores at least the identifier of the key tag of the stored key set. The memory of the key container can include a lockout list  
10 identifying an unauthorized access device or an unauthorized user. The memory of the access device can record the approximate time that a successful access was made and/or the approximate time that a key tag was returned to the key tag storage area. The memory of the access device can include stored privileges.

The key container can have an open position in which the key set storage area can be  
15 accessed and a closed position in which the key set storage area cannot be accessed. Removing the key set from the key storage area can prevent the key container from being changed from the opened position to the closed position.

In particular implementations, the key management system includes a central computer and an associated database for administering the system. The central computer  
20 allows an administrator to set each user's access privileges and to track the user's access activity. The system can allow the user to log into the central computer to reestablish his expired access privileges. The user seeking to access a key container can use his access device to communicate his identifying information and to select one of a predetermined group of codes corresponding to the purpose of the access. The information stored in the  
25 memory of an expired access device can be automatically uploaded to a data base when the access device is reauthorized. The key container can be capable of communicating with the key set when the electrical contact portion of the key tag is placed to complete an electrical circuit in the key container.

According to another implementation, a key management system for managing  
30 access to keys has an organizational hierarchy with at least three levels having multiple

entities within each level, including, in descending hierarchical order, a first dealer group level, a second dealership level and a third department level. Each key is assigned to one entity at any level. The system includes a permissions data structure for assigning permissions to various users of the system in which permissions for any particular user can  
5 be assigned, on a level by level basis, to all entities, fewer than all entities or no entities. The system compares the particular user's assigned permissions against the key's assignment to determine whether the user is authorized to access the key.

The system may further include a zeroth organization level hierarchically above the first, second and third levels. Assignment of privileges to all entities of any level can  
10 automatically confer privileges to all entities of any hierarchically lower level.

### **Brief Description of the Drawings**

Fig. 1 is a schematic view of a key management system as configured for a car dealership implementation, which includes a key pad assigned to a user, a remotely located  
15 key container for securing vehicle keys, a central computer that administers the system, and other components.

Fig. 2 is a flow chart showing operational aspects of the key management system from the standpoint of a typical user, such as a salesperson.

Fig. 3 is a flow chart showing operational aspects of the key management system  
20 from the standpoint of another class of user, such as a lot attendant.

Fig. 4 is a flowchart showing operational aspects of making an access to the key container using the key pad.

Figs. 5-7 are flow charts showing operational aspects of the key management system related to the central computer, programming base and key pad according to the functions  
25 available for the salesperson.

Figs. 8-10 are flow charts showing operational aspects related to the central computer, programming base and key pad according to the functions available to an administrator.

Fig. 11A is a perspective view of an exemplary key container in an unlocked position  
30 which shows the key set storage area and a representative key tag.

Fig. 11B is a drawing showing a user removing and replacing a key set from the key container of Fig. 11A.

Fig. 12 is a schematic view showing an implementation of the system configured for use by multiple dealerships belonging to a single "group," and among various departments  
5 within each dealership.

Figs. 13-18 are exemplary screen displays showing operational aspects of the key management system.

Fig. 19 is a perspective view of an alternative key container, which is shown in an unlocked position similar to Fig. 11A, but with the key tag in place.

10 Figs. 20 and 21 are sectional views showing a left side elevation and a front side elevation, respectively, of the key container of Fig. 19 in a closed position.

Figs. 22 and 23A are sectional views showing additional front side elevations of the key container of Fig. 19 showing the movable portion being urged upward from the closed position prior to being released and in the open position after release, respectively.

15 Fig. 23B is a sectional view showing a left side elevation of the key container in the open position, with the key tag in place.

Fig. 24 is a sectional view showing a left side elevation of the key container of Fig. 19 in a partially open position.

20 Fig. 25 is a schematic view of a power conservation portion of a key container circuit.

Fig. 26 is a schematic view of the key management system of Fig. 1 showing additional features.

Fig. 27 is a diagram showing another example of the administration of access privileges among users of the system.

25

### **Detailed Description**

Described below are implementations of an asset management system. In one implementation, the system is configured for management of physical assets and (1) allows article(s) necessary to access a locked object or area, which would include a key or keys, to  
30 be securely stored near the object or area in a locked container, (2) allows access to the



container with an electronic access device by an authorized user, and (3) allows tracking of access activity.

### *System Overview*

An implementation 10 of the key management system is shown schematically in Fig. 1. In the system 10, the articles of interest are keys to motor vehicles, such as the illustrated vehicle keys 12 for a vehicle V. The vehicle keys 12 are secured at or near the respective vehicle in a "key box" or key container 14 that is locked with an electronic lock. The vehicle V is presumably unattended, so a user seeking to access the vehicle in a normal fashion (1) unlocks the key container 14, (2) removes the vehicle keys 12 from the key container 14, (3) uses one of the vehicle keys 12 (or an attached conventional electronic key fob 13) to unlock the vehicle if the vehicle is locked, and (4) if desired, uses the one of the vehicle keys 12 to start the vehicle.

The user unlocks the key container 14 by linking a pre-programmed electronic access device with the key container 14 and successfully demonstrating that the user is authorized to make access to the key container 14, based on, e.g., one or more of the following: the user's identity, the user's pre-assigned privileges, the user's prior activity, the time of day, etc. In the illustrated implementations, the access device is a small, battery-powered, microprocessor-based unit with a memory, a display, a key pad that allows the user to enter information, and input/output capability for receiving programming instructions or communicating information, such as sending a user's PIN to a linked key container 14 that the user wishes to access. One specific access device is the key pad 16 of the type illustrated in Fig. 1.

Assuming that the user's request to access the key container 14 is authorized, the electronic lock of the key container 14 is unlocked and information about the access is recorded in memory, which may include a memory in the key pad 16 and/or a memory in the key container 14. At periodic intervals, e.g., the end of a salesperson's shift, the information stored in memory can be uploaded to a central computer 21 for managing and tracking access activity.

The central computer 21 is programmed for use in administering the system 10, including assigning privileges to different classes of users, updating information about

current inventory to be tracked, tracking activity of key pads 16, users and vehicles, and allowing certain classes of users to generate and view reports.

The central computer 21 is linked to a database that stores information for administering the key management system. As illustrated in Fig. 1, the information can be stored in and retrieved from a networked database, such as the database 27 linked through a server 26 via a public network, such as the internet, or a private network.

The central computer 21 would typically be located at a convenient but secure site at the dealership, e.g., in the dealership's central offices. If an access device such as the key pad 16 is used, there is also a programming base 22 connected to the central computer 21 that provides an interface for connecting the key pad 16 and the central computer 21 together to exchange information.

If desired, one or more additional computers, such as the remote computer 24, can also be linked to the system via the internet or other network. For example, the dealership owner may have one such remote computer 24 located at her residence. There may also be implementations in which multiple central computers and/or multiple databases (located on-site or remotely) are networked together to provide a coordinated management system, e.g., in the case of a large auto group with multiple dealerships at different locations.

Additionally, an optional system administration channel may be provided, such as a telephone link 28 to live customer support and/or a voice-activated server.

In some implementations, such as is illustrated in Fig. 1, the vehicle keys 12 will be attached to a key tag 18 that includes an electronically stored identifier. When the system is initially configured to include the vehicle V in inventory, unique identification information about that vehicle (e.g., the vehicle's VIN) is recorded in the database associated with the central computer 21 to correlate the vehicle V with the identifier of the assigned key tag 18. The programming base 22 can be configured to include an appropriate reader for the key tag 18. Preferably, the key tag 18 is physically attached to the vehicle keys to form what is referred to herein as a "key set," such as the illustrated key set 20.

Additional details are described below.

### *Operation*

Operation of the system 10 is described below in connection with an exemplary implementation at a vehicle dealership. At any time, the dealership has an inventory of vehicles under its care, which may include both new and used vehicles being offered for sale, as well as vehicles owned by others that have been left at the dealership for service. Vehicles may need to be accessed several times over the course of each business day, e.g., to move them to other locations, to allow potential customers to test drive them, to view their interiors, etc. In a large dealership, the vehicles may be distributed over an extensive area, so keeping each vehicle's keys securely stored, but at a location near the respective vehicle, is desirable.

### *Salesperson*

In the case of its sales force, the dealership desires to give each authorized salesperson privileges to access some or all of the vehicles being offered for sale without unduly interfering with the sales process. There may be reasons, however, to restrict a salesperson's ability to access vehicles, e.g., the salesperson is no longer an employee of the dealership, the salesperson's work shift is over, the salesperson has exceeded a maximum number of vehicle accesses for a given period, or the salesperson is authorized to sell only certain vehicles (e.g., only used vehicles or only a particular make of vehicles).

Fig. 2 is a flowchart showing the steps taken by a typical salesperson over the course of her shift. In step 100, the salesperson logs into the central computer 21 and "checks out" any available key pad 16, which is programmed with appropriate privileges for her status, as described below in greater detail in connection with Figs. 5 and 6. The salesperson then uses her assigned key pad 16 to make an access to a vehicle, which is probably at a location remote from the central computer (step 200). Following each access, the salesperson normally would then return the key set 20 to the key container 14 and close it (step 300), which returns the key set 20 to a secured state. This process is repeated over the course of the salesperson's shift (step 400). At the end of her shift, the salesperson normally returns to the central computer 21 and "checks in" her assigned key pad 16 (step 500), which allows the information about her activity to be uploaded to the system.

*Lot attendant*

Fig. 3 is similar to Fig. 2, and the steps that are the same as in Fig. 1 are identified with the same reference number. In Fig. 3, however, the steps shown are those taken by a typical lot attendant, e.g., at the end of the business day when the key set 20 from each vehicle is collected from each respective key container 14 for storage at a secure location. This precaution can be taken if the dealership desires not to leave the key sets 20 in the key containers while the dealership is unattended.

As in Fig. 1, the lot attendant checks out a key pad 16 (step 100), and uses it to access one of the key containers 14 and retrieve the respective key set 20. The retrieved key set is collected (step 410), and the process is repeated until all desired key sets have been retrieved (step 420). The retrieved key sets are stored in a secure location (step 430), and the lot attendant's key is checked in (step 500).

*Key Pad/Key Container Interaction*

Fig. 3 is a flowchart showing the sub-steps of step 200, i.e., the steps involved in making an access. The user (which could be a salesperson, a lot attendant or another class of user) has decided to request access to a vehicle having a locked key container 14. The user validates her identity, e.g., by entering her PIN on the key pad 16 (step 210). The key container 14 can be programmed to participate in a challenge-response or other similar scheme with the user and key pad 16 as part of the validation or authorization of a user's request to gain access. Examples of such a scheme are described in commonly-owned International Application PCT/US02/13653 and U.S. Patent Application 10/363,938.

Assuming that correct identifying information has been entered, the user is then prompted to enter a usage code corresponding to the intended reason she is seeking access (step 212). Exemplary usage codes could include one or more of the following: sales demo, service, body shop, PDI (Preparation, Detail, Inspection), overnight, aftermarket, or retrieving key for central storage.

In step 214, the user is then prompted to link her key pad 16 to the key container 14, in this case by physically connecting the key pad 16 to the key container 14. When an electrical connection between the key pad 16 and the key container 18 is established (step 216), the key container "wakes up" based on electrical power provided from the key

pad 16 to circuitry in the key container 14. In other embodiments as described elsewhere, the key pad establishes a wireless communications link (such as, e.g., via IrDa, RF or any other suitable wireless communications protocol) with the key container 14, and the key pad does not supply power to the key container.

5           In step 218, it is determined whether the key pad 16 is authorized to make the requested access. It is possible to prevent a user from making an otherwise authorized access (i.e., one within the privileges programmed for the user's key pad 16) by identifying the user on a "lock out" list stored in the key container 14.

          If the access is not authorized, the key pad 16 indicates this result (e.g., via a  
10   displayed and/or audio message) (step 220), and the key pad 16 displays its main menu (step 222).

          If the access is authorized, information about the access is recorded in the memory of the key container 14 (step 224) and in the memory of the key pad 16 (step 226). The information recorded in the memory of the key container 14 is stored in the form of an audit  
15   trail and may include the user's identification, the usage code, the date and time of the access, and the identification of the key tag 18, if present. The information recorded in the memory of the key pad 16 would usually include identification of the key tag 18 corresponding to the key set 20 in the key container 14, the date and time of the access and the usage code.

20           Following step 226, the key container 14 is unlocked to allow access to the key set 20 (step 228). The user may then use the key set 20 to unlock the vehicle.

          If the user is determined to have lot attendant privileges (step 230), such as indicated by entering the appropriate usage code in step 212, the process returns to step 214 and she is prompted to connect her assigned key pad to the key container 14 for the next vehicle. In  
25   this way, the responsible lot attendant may access each key container 14 for multiple cars and collect the respective key sets quickly, e.g., at the end of the business day. The process can be designed to require the lot attendant to reauthorize herself (e.g., by reentering her PIN) after a given time period (e.g., every 10 minutes) and/or after a predetermined number of accesses (e.g., after every 10 accesses).

*Checking In/Checking Out a Key Pad*

Figs. 5-7 are flow charts showing the steps involved in "checking out" or "checking in" a key pad 16.

According to Fig. 5, the user uses the central computer 21 to access the system program. In step 110, the user is prompted for identifying information, such as her name and PIN code. In step 112, it is determined whether the user is authorized. If the user is not authorized, the process is halted.

If the user is authorized, the user's record is retrieved from the database and a menu of options available to the particular user is displayed (step 114). For example, if the user is a salesperson, the displayed options may include "Check out Key Pad" (step 116), "Check in Key Pad" (step 118) and "Log out" (step 120). If the user selects "Log out" (step 120), the process is halted.

If the user selects "Check out Key Pad," the process proceeds to the steps shown in Fig. 6. In step 122, it is determined whether the user has exceeded a number of checked out key pads limit. The system may be programmed to allow the user to have more than one key pad 16 checked out at one time to account, e.g., for occasions when the user may have forgotten to return the key pad 16 at the end of her previous shift or beginning of the current shift. If the user has reached the checked out key pads limit, a suitable message is displayed (step 123), the check out process is halted, and the process returns to step 114.

If the user has not reached the checked out keypads limit, she is prompted to place a key pad 16 in the programming base 22 (step 124). In step 126, the user selects a key pad 16 and links it to the programming base 22, e.g., by physically or wirelessly connecting it to the programming base 22. In step 128, any previous activity information stored in the key pad 16 is uploaded to the database and the key pad 16 is activated for the particular user in accordance with the user's predetermined privileges from her record. Advantageously, the user can select any one of a number of available key pads, since the selected one will be reprogrammed for her according to her identity and privileges. Alternatively, some or all users may retain possession of specific key pads 16 that have been assigned to them, but will still need to follow generally the same steps for periodic reauthorization.

In step 130, the user's record is updated to reflect that the assigned key has been checked out to the user.

Following step 114 in Fig. 5, if the user selects "Check in Key Pad," the process proceeds to Fig. 7. In step 502, the user is prompted to link her checked out key pad 16 to the programming base 22. After the key pad 16 is linked, any access information stored in its memory is uploaded to the database (step 504). In step 506, the key pad 16 is deactivated, and the user's identity and privileges may be erased from memory. In step 508, the user's record is updated to reflect that she checked in the key pad 16. In step 510, check in is completed and the process returns to displaying the menu (step 114 of Fig. 5).

According to an alternative check in procedure, user log in is not required. Rather the key pad 16 is linked to the programming base 22 and the system is instructed to check in the key pad 16.

#### *Administrator Functions*

Certain functionality is reserved for system administrators. Figs. 8-10 are flow charts showing the steps associated with some of these functions.

In Fig. 8, the administrator uses the central computer 21 to change vehicle inventory information, in this case to add a new vehicle. It is also possible, of course, to follow a similar procedure to reflect that a vehicle is no longer in inventory (e.g., after it is sold), which would include "unassigning" the key tag 18.

In step 800, the administrator is prompted to enter her identification information, e.g., her username and password. In step 802, it is determined whether the administrator is authorized. If the administrator is not authorized, the process is halted.

In step 804, a menu of administrative options available to the administrator is displayed, such as "Import Vehicles" (step 806), "Key Tag Assignment" (step 808) and "Logout" (step 810). If "Logout" (step 810) is selected, the process returns to the original login screen (step 800).

If "Import Vehicles" (step 806) is selected, the process proceeds to the steps shown in Fig. 9. It would, of course, be possible to manually enter the vehicle information rather than importing it. In step 812, the administrator is prompted to select or enter information identifying a third party database, such as a customer relationship management (CRM)

database or a dealership management database (DSM), from which information about the new vehicles to be added to the dealership inventory is to be retrieved. In step 814, the computer 20 attempts to establish a connection with the desired third party database. If efforts to make the connection are unsuccessful, the process is halted.

5        If the connection is established, the process proceeds to step 816, and data corresponding to the desired new vehicle is downloaded from the third party database to the database for the system 10.

10        If "Key Tag Assignment" (step 808) is selected, the process proceeds to the steps shown in Fig. 10 to allow the administrator to assign a key tag 18 to the vehicle keys 12 for a particular vehicle. The administrator is prompted to choose between looking up the key tag 18 by typing in the serial number of the key tag (step 818), or scanning the key tag 18 electronically to determine its serial number (step 820). Scanning may be accomplished using a key tag reader (not shown) connected to the central computer 21.

15        If the key tag is currently assigned, information for the currently assigned vehicle is displayed (step 822). In step 824, the administrator is prompted to select a vehicle to which the key tag is to be assigned. In step 826, the new key tag assignment information is stored in the system database.

#### *Usage Among Various Classes of Users*

20        Fig. 12 is a schematic diagram showing how the system 10 may be configured to provide and restrict privileges according to a user's class within an organization, in this case the user's department within the dealership or the user's role within the larger dealership group.

25        As illustrated, there is an overall dealer group 80 that includes a first dealership 82 and a second dealership 84. The first dealership 82 has five departments: a Toyota New Cars Department 86, a Toyota Used Cars Department 88, a Lexus New Cars Department 90, a Lexus Used Cars Department 92, and a Service Department 94. The second dealership has three departments: a Chevrolet New Cars Department 96, a Chevrolet Used Cars Department 98, and a Service Department 102.

30        A first dealership 82 salesperson may have privileges to access vehicles in only a single sales department, such as the Toyota New Cars Department 86, or in multiple



departments, such as the Toyota New Cars Department 86 and the Toyota Used Cars Department 88. Similarly, an employee of the service department 94 may be granted privileges only to access vehicles assigned to that department.

5 A first dealership 82 administrator, however, may be granted privileges across as many as all five departments. Similar assignments of privileges to one, more than one or all departments are possible in the second dealership 84.

In the case where the first dealership 82 and the second dealership 84 are related as members of the auto group 80, there may be a class of users who are authorized for access across one or more departments in both dealerships, such as the owner (privileges to access  
10 vehicles in all departments) and the new car sales manager (privileges for the new car departments 86, 90 and 96). Other combinations of privileges are, of course, possible.

Such privileges or "permissions" may be implemented in various ways. For example, in the scenario above in which the user's class within the organization is the user's department, the key containers for use in that department can be identified as such within the  
15 system. In other words, the Toyota New Cars department can have a number of key containers that are assigned to that department, which would be identified in the database. A salesperson belonging to the Toyota New Cars department typically would have privileges to access all Toyota New Cars key containers, subject to regular authorization (e.g., providing his PIN upon requesting access), periodic normal expiration (e.g., after the end of the user's  
20 shift) or special expiration (e.g., user now on a lock-out list), of his access privileges. Thus, a Toyota New Cars salesperson would have privileges that match or are consistent with the privileges information stored in a Toyota New Cars key container.

Another example is shown in Fig. 27. Fig. 27 presents the possibilities for user permissions to access vehicles within the system, which is depicted as a hierarchy in this  
25 example, of a zeroth level (the organization, i.e., Ann's Auto Empire), a first level (dealer groups, i.e., the Portland Group and the Beaverton Mall Group), a second level (dealerships, i.e., Honda, Chevrolet and Ford dealerships of the Portland Group, and VW, Ford Truck and Used Car dealerships of the Beaverton Mall Group) and a third level (departments, i.e., New, Used, Body, Rentals and Service, as indicated for the various dealerships).

The cross-hatched entities represent the privileges assigned to a particular user (or a class of users). In this example, the senior sales staff of the Ford Truck Dealership of Ann's Auto Empire are assigned privileges entitling them to access all vehicles for sale at the Beaverton Mall Group, as well as to Ford Dealership vehicles for sale at the Portland Group.

5 This may be done, e.g., because senior sales staff of one dealership are expected to sell across brands within their dealer group, and to sell to affiliated brands of other dealer groups within the organization (i.e., because Ford cars are affiliated with Ford Trucks).

Thus, for the Beaverton Mall Group, the senior sales staff have privileges allowing access to keys for vehicles assigned to the New cars department of the VW dealership, the

10 New cars department of the Ford Truck dealership, and the Used cars department of the Used Cars dealership. The senior sales staff do not have privileges, however, to the Service departments of these dealerships within the Beaverton Mall Group.

Considering the Portland Group, the senior sales staff have privileges only allowing access to keys of vehicles assigned to the New cars department of the Ford Dealership, but

15 not to the Service, Body and Rentals departments of that dealership.

#### *Exemplary Screen Displays*

Figs. 13-18 are exemplary screen displays showing the administration of the system with respect to the privileges assigned to particular classes of users. These displays may be available on the central computer 21 and/or on one of the remote computers 24.

20 Fig. 13 is a screen display available to a corporate administrator for a dealership showing the user configuration record for one of the dealership's employees, Nellie Frost. As indicated, Nellie belongs to a class called "local administrator" at Lot 2. Her login ID and password are indicated in the upper right hand corner.

According to the checked boxes at the left hand portion of the screen, Nellie is

25 entitled to access only Lot 2 vehicles assigned to the "new" and "used" categories. At the lower right hand portion of the screen display, the checked boxes indicate that Nellie's privileges, for Lot 2, include: editing all records, programming devices and viewing reports.

Fig. 14 is a screen display available to Nellie Frost as a local key administrator, showing the user configuration record for another employee, Frank Snipes. As indicated,

Frank Snipes is the Sales Manager for Lot 2, and he has been assigned privileges to access Lot 2 vehicles in the "new" category, to view reports and to view screens (without editing).

Fig. 15 is a screen display available to Nellie Frost as she sets the privileges available to a new employee, i.e., Salesperson 1 at Lot 2. As illustrated, Salesperson 1 has been  
5 granted privileges to access vehicles at Lot 2 in the "new" category from Monday through Friday during a shift from 8:00 (8:00 am) to 17:00 (5:00 pm). Salesperson 1's PIN code has been set as indicated to "1122." According to the screen display, Salesperson 1 has one key pad, i.e., with the identifier 645598, checked out.

Fig. 16 is a screen display available to Nellie Frost as she sets the privileges available  
10 to another new employee, i.e., Service Technician 1 at Lot 2. As illustrated, Service Technician 1 has privileges to access vehicles at Lot 2 in the "service" category from Monday through Friday during a shift from 6:00 (6:00 am) to 15:30 (3:30 pm), but only up to maximum of 25 vehicles per assigned key pad. Service Technician 1's PIN code has been set as indicated to "4321." According to the screen display, Service Technician 1 has one  
15 key pad, i.e., with the identifier 645599, checked out.

Fig. 17 is a screen display showing the user configuration for Tom Smith, the dealership owner. Tom Smith divides his time among three different lots, and thus his access privileges extend to each of those lots as indicated. Tom Smith may access vehicles at all hours and on all days. The lower right portion of the screen display indicates that Tom  
20 Smith has two key pads 16 currently in use, perhaps because he inadvertently failed to check one in after a previous use.

If Tom Smith happened to arrive at Lot 3 without remembering his assigned key pad, he could check out another key pad because he is not limited to a maximum number of key pads.

25 Fig. 18 is a screen display showing the user configuration for Jim Jones, which has been reprogrammed in anticipation of a special event, e.g., a sale of vehicles pooled from several lots. Jim Jones, who customarily works only in Lot 1, has been granted privileges to access new vehicles from Lot 2 and Lot 3 for the sale during the time shown. Following the sale, the key administrator can easily reprogram Jim Jones' privileges for normal access to  
30 Lot 1.

*Reports*

As indicated, the system 10 allows various types of reports to be generated, provided the requesting person has appropriate privileges. Any such report can be generated in a printed or electronic form, and can be used on-site or automatically transmitted to a remote location, by e-mail or other form of transmission.

For example, an administrator can generate a report from the database of activity from all users (or "key holders"), or some class of users. This report would normally include, for a desired time frame, the user's identifying information, identification of the assigned key pad, the vehicles that were accessed, the date and time of the access, and the usage code associated with the access.

It is also possible to generate a recent vehicle activity report sorted by the vehicles in inventory. This report provides information on the last several accesses of each vehicle, such as which user made the access, the time and date the access was made and the purpose of the access. This report might be used, e.g., in tracking unreported damage to a vehicle that is discovered at a later time.

For any specific vehicle, a similar report showing information about the last several accesses is available in the field, if authorized, by linking a key pad 16 to the key container 14 and requesting it. The report is viewed on the key pad 16 and/or on the key container, depending upon the particular implementation.

Other report formats include:

- a vehicle history report for one or more vehicles showing the stored access information, which can be sorted by time, vehicle ID or purpose (usage code)
- a key pad assignment report showing which key pads were assigned to which user and over what time period
- a key pad programming report showing when and by whom key pads were checked out and checked in
- a key pad exception report showing key pads that have not been assigned/had activity recently, and key pads that have been assigned but have not been checked in

- an outstanding vehicle keys report that allows an administrator to verify that all vehicle keys have been returned to central storage, e.g., at the end of the business day. If a vehicle appears in this report, the respective vehicle keys have not been returned. Similarly, an outstanding key pad report lists the keys that have not been checked in
- an inventory report showing all key containers, key pads and key tags by, e.g., their respective serial numbers and status
- a reconciliation report showing key tags that remain assigned to vehicles that have been sold and vehicles to which no key tag has been assigned
- a user configuration report showing the complete set of assigned privileges for a specific user or a group of users.

The above report formats are exemplary only, and other report formats would of course be possible.

#### *Major Components*

Additional details regarding major components of the system 10 are described below.

##### *Key Pad*

The access device or key pad 16 may be a device similar to the present assignee's DisplayKEY or a similar device, except that it may be programmed to expire after a shorter operating period (e.g., the length of a shift in the case of a key pad 16 assigned to a salesperson) and it may have non-rechargeable batteries. Each key pad 16 is usually assigned a unique serial number that is recorded in the database.

In the illustrated implementations, the key pad 16 is linked with other devices to exchange information via a physical electrical connection, i.e., electrical contacts of the key pad 16 physically contact and form an electrical connection with corresponding contacts of the key container 14 or of the programming base 22. Other linking technologies are also available, including those that do not require a physical connection between the devices, such as infrared, radio frequency, etc.

##### *Key Container*

One specific implementation of the key box or key container 14 is shown in Fig.

11A. The key container 14 has a key set storage area 30 capable of accommodating the key

set 20, which as shown in Fig. 1 may include one or more vehicle keys 12, the key tag 18 and its attachment, and, in some cases, the conventional electronic key fob 13 (or "remote") provided with the vehicle keys 12.

5 The key set storage portion 30 is defined in a movable portion 32 of the key container 14. The movable portion 32 is released to slide downwardly as indicated by arrow A when the key container 14 is unlocked.

The key container 14 has a key pad interface portion 34 shaped to receive and establish electrical contact with the key pad 16. In the illustrated implementation, the keypad interface portion is defined in a lower end 36 of the movable portion 34.

10 The key container 14 includes a microprocessor-based circuit that includes a memory and a solenoid that is selectively controllable to "unlock the lock," i.e., to release the movable portion 32. Motors, magnets or other similar devices could be used in place of the solenoid. The circuit in the key container 14 is normally configured to receive power from a linked key pad 16, so no separate power source within the key container 14 is required.

15 In some implementations, and possibly if infrared, RF or other wireless communication capability between the access device and the key container 14 is provided, there may be a dedicated power source for the key container circuit.

The key container 14 has an attachment portion for attaching the key container 14 to a secure object. In the illustrated implementation, the attachment portion is a hanger 38  
20 shaped to slide over the edge of the glass in a partially open vehicle window to support the key container 14. The window can then be closed to prevent a thief from simply removing the key container from an unattended vehicle.

Other implementations of the key container 14 may have a door or other structure that selectively allows access to the key set storage portion 30, instead of the drawer-like  
25 arrangement shown in the figures.

#### *Key Tag*

Also shown in Fig. 11A is a specific implementation of the key tag 18. The key tag 18 has an identifier element 40 that can be electronically read and an eyelet 42 to allow the key tag 18 to be attached to the vehicle keys 12. Although not shown, the

attachment between the key tag 18 and the vehicle keys 12 is preferably tamper-evident, but sufficiently strong to avoid the efforts of a casual intermeddler.

One suitable identifier element 40 is the iButton® available from Dallas Semiconductor. A suitable reader for reading the serial number from the identifier  
5 element 40 is also available from Dallas Semiconductor.

In the illustrated implementation, presence of the key set 20 in the key container 14 is detected by presence of the key tag 18. Specifically, there is a key tag receiving portion 44 defined in the key set storage portion 30 of the key container. When the key tag 18 is received in the key tag receiving portion 44, the identifier element 40 completes a circuit in  
10 the key container. Fig. 11B is included to show a user removing and replacing the key set 20 by sliding the attached key tag 18 out from and into, respectively, the key tag receiving portion 44

The key container 14 can be configured to allow it to be locked only when the key set 20 is present in the key container 14. In the illustrated implementation, the movable  
15 portion 32 cannot be returned to its closed position unless the key tag 18 is received in the key tag receiving portion 44. In some situations, such as during shipping, the key tag receiving portion may be loaded with a dummy or place holder key tag 16 to allow the key container to be closed.

#### *Additional Key Tag Features*

20 If desired, the system 10 can be modified to provide for tracking of key tags. In one implementation, each key tag can be tracked to determine the time when it was returned to the respective key box. One suitable identifier element for a trackable key tag would be, e.g., the iButton® DS1904 identifier which includes a real-time clock in addition to the basic memory and power source present in a base model iButton® identifier. In such an  
25 implementation, data relating to the tracking of key sets would be recorded in the memory of the key container.

In other implementations, the key tag may be configured as the assigned entity, instead of or in addition to the key container. In these implementations, the key tag would record some or all of the information relating to tracking of the key sets and access  
30 privileges. In these implementations, similar to the key container implementations above,

the key tag would be programmed to grant access, i.e., by unlocking the lock of the key container, if the user's privileges as communicated through the access device are consistent with the privileges assigned to the key tag. The key tag would include an updatable memory, and possibly other electronic components, such as a microprocessor. Suitable devices include, e.g., the iButton® NV RAM, EPROM, EEPROM identifiers, as well as other compact solid state memory devices.

For some implementations, the key tag can be configured to communicate wirelessly with the key container. Communication between the key tag and the key container may take place when the key tag is within the key container, or when the key tag is within close proximity of the key container. The communication may be restricted to simply the identifier of the key tag, or may include communication of all necessary tracking and access privileges information. The key tag can include an RF identification tag for such communication, and the key container can include an RF transceiver, including a transceiver that provides power to the key tag.

#### *Alternative Key Container*

Figs. 19-24 show various views of a key container 314 according to an alternative implementation.

Among other features, the key container 314 has a mechanical detent 341 that operates to maintain a movable portion 332 of the key container in desired positions, such as in an open position as shown in, e.g., Fig. 19. The key container 314 also has a lightweight but tamper-resistant construction to frustrate efforts of someone attempting to pry open or bend the key container to gain access. Additionally, the key container is maintained in a locked condition by an electromagnet that holds the movable portion 332 in the closed position until an authorized request for access is made.

Referring to Fig. 19, the key container 314 is shown in the open position with a key tag 318 inserted in a key tag receiving portion 344. Fig. 23B shows a side elevation of the key container 314 of Fig. 9 in the open position. At a lower end 336, there is an IR lens 335 positioned for receiving/exchanging infrared signals with an adjacent device, such as an enhanced key pad 16 or other suitably equipped access device. Within the key container 314, light signals are conveyed through a light pipe 337, which is partially visible



in Fig. 19 and extends from the IR lens 335, along an interior rear surface of the movable portion 332 and to a suitable receiver or transceiver (not shown).

As seen in Fig. 19, the key container 314 has a housing 315 into which the movable portion 332 can be slidably retracted and locked in the closed position. The housing 315 has a bulged portion 317 on its front surface. The bulged portion 317 allows a construction that assists in preventing unauthorized access to a key set or other asset stored in the a key set storage area of the movable portion 332, as is described below in greater detail.

When the key tag 318 is removed from the key tag receiving portion 344, the detent 341 mechanically coupled to the key tag receiving portion 344 is extended, causing it to protrude from the movable portion 332, as shown, e.g., in Fig. 24. With the detent 341 extended, the movable portion 332 cannot be returned to the closed and locked position shown in Fig. 20. With the detent 341 extended, the movable portion 332 can be moved upward by hand to a partially open position, e.g., as shown in Fig. 24, if desired. As can be seen in Fig. 24, the extended detent 341 contacts a stop or recess, thus preventing the movable portion 332 from further travel in the direction of arrow A. The partially open position can be used, e.g., during inclement weather to prevent precipitation from entering the key container 314.

Referring to Fig. 20, a circuit 345 and its power source, e.g., a battery 347, are shown schematically within an upper section of the movable portion 332. The circuit 345 functions to retain the key container 314 in a locked state until an authorized unlock request signal is received. In the illustrated implementation, the circuit 345 includes additional components, e.g., at least a receiver, for receiving such signals via infrared or other wireless form of transmission.

The operation of the locking mechanism is shown with reference to Figs. 21-23. In the illustrated implementation, the locking mechanism includes a pair of solenoids with opposed movable members 351 surrounded by coils 356. The solenoids are attached to the movable portion 332. The interior of the housing 315 has a corresponding pair of retaining members 353 positioned to receive the movable members 351, thus securing the movable portion 332 in the closed and locked position as shown in Figs. 20 and 21.

In operation, an authorized user seeking to unlock the key container 314 first enters his PIN on the keypad of his enhanced key pad and then aligns the key pad with the IR lens 335 on the lower end 336 and initiates an IR communication. If the communication is successful, a message is displayed instructing the user to push upwards on the lower end

5 336.

Referring to Fig. 22, the user then urges the lower end 336 of the movable portion 332 upward, which in turn causes outer ends 355 of the movable members 351 to slide against ramps 357 until the movable members 351 are brought into contact with each other. The coils 356 have an inductance that changes depending on the positions of the

10 movable members 351. The circuit 345 is configured to sense inductance in the coils 356, and based on a predetermined change in inductance, to trigger power to be supplied from the battery 347 to energize the coils 356. When the coils 356 are energized, the movable members 351 become magnetized and attract each other by magnetic force, and the movable portion 332 is released and allowed to open, as shown in Fig. 23A.

15 Advantageously, the coils 356 need only be supplied with power for a very a short period, e.g., about 3 seconds or even as short as about 1 second. Thus, power consumption is reduced, which allows the life of the battery 347 to be preserved.

As best shown in Fig. 23A, the movable members 351 can have flanged outer ends 357 to prevent efforts to force the movable members 351 together and defeat the lock

20 by simultaneous impacts applied at their outer ends.

The housing 315 and the movable portion 332 can each be constructed with multiple layers of material that are interleaved with each other when the key container 314 is closed and locked. As best shown in Fig. 20, the housing 315 can have multiple spaced layers 359, and the movable portion 332 can have multiple spaced layers 361. When the movable

25 portion 332 is in a closed and locked position as shown in Fig. 20, the layers 359 and the layers 361 are alternately interleaved with each other.

In the event that someone attempts to break into the key container 314, e.g., by attempting to pry apart the housing 315 and the movable portion 332, the relatively thin layers 359 and 361 will tend to bend together, preventing easy separation and/or access to

30 the secured articles.

In typical configurations, the key container 314 has a hanger 338 for supporting the key container from the window of a vehicle. The hanger 338 may be formed with slots 339 as shown, e.g., in Fig. 21, to provide increased resistance to vandalism, e.g., by efforts to cut the hanger 338 and remove the 314 from the vehicle.

- 5           The housing 315 and/or the lower end 336 may be covered in resilient material, such as rubber or other similar material, to reduce damage to vehicles and users.

#### *Power Conservation*

The circuit 345 may be configured to conserve power in the key container 314. A power conserving portion 400 of the circuit 345 is shown schematically in Fig. 25.

- 10           Referring to Fig. 25, there is a network of a diode 406 along a diode branch 408 connected in parallel with the coils 356 of the solenoids along a solenoid branch 412. Power is provided across the network by a power source, e.g., the battery 347, which is rapidly cycled on and off by a switching transistor 404.

- 15           When the switching transistor 404 is closed, such as in response to an authorized access request, current flows through the coils 356 and energizes the solenoid to move the movable members 351. The diode 406 prevents current from flowing through the diode branch 408.

- 20           When the switching transistor 404 is opened and the supply of power is stopped abruptly, idling current continues to flow through the solenoid branch 412 and the diode branch 408 in the direction of the arrow, which prevents the field of the coils 356 from collapsing.

- 25           As a result, the power consumption of the solenoid can be controlled by varying the duty cycle of the switching transistor 404. This allows the application of high power to magnetize the movable members 351 when the switching transistor is first turned on and the application of low power later in the open cycle to hold the elements together. Under typical operating conditions with this approach, as much as a 50% power savings can be realized.

#### *Open Architecture*

- 30           The system 10 can be implemented for use with open architecture aspects, yet preserve the necessary level of security for system integrity. For example, one or more of the access devices or key pads 16 may be a personal digital assistant (PDA), mobile phone or

other personal information device programmed to additionally serve as an electronic key, referred to herein as an "enhanced" keypad. The system may include both enhanced key pads and standard key pads. If such an enhanced key pad has an open architecture format, such as in the case of Palm® devices and other devices, additional measures are desirable to  
5 protect against unauthorized use of the system.

As used herein, the term "open architecture" refers to a property of the access device that allows any application or user to inspect, add, delete, modify, and duplicate other applications and their data on the device. An example of this is the common PC. A common example of a "closed architecture" device would be a simple hand-held calculator,  
10 where all functions are built-in. The term "open" implies that major components of the system, communication protocols and interfaces are designed according to published standards that allow integration with other systems and components.

Commonly-owned International Application PCT/US02/13653 and U.S. Patent Application 10/363,938 describe methods and apparatus for implementing a secure access  
15 system with electronic locks and open architecture keys and are incorporated herein by reference. The described examples are for real estate lockbox secure access system, but the same principles apply in other implementations, such as for key management in a car dealership.

Essentially, the commonly-owned applications describe algorithms to allow  
20 relatively secure exchange of data among electronic keys, electronic locks and a central authority, which may include one or more computers. As described, the electronic key can be a PDA programmed to serve as a key and intended for use by an authorized user. The electronic lock can be a lockbox securing conventional keys to a residence or other property. The central authority oversees the system, including administration of user access privileges.  
25 Access privileges are programmed to expire at predetermined times and thus require users to reauthorize themselves by renewing their privileges to continue use of the system. For security, selected communications are encrypted.

As described, the algorithms can include communicating a parameter, together with other information, which is received and stored in a memory of the electronic key. The  
30 identity of the parameter and its exact location in the memory of the electronic key, however,

are not generally known or determinable. In normal use by an authorized user, the stored parameter is included in communications of information to the lockbox and to the central authority, thus verifying to the lockbox and the central authority, respectively, that the key is authorized.

5           Should another attempt to defeat the system by making a copy of the key memory, however, he will generally not be successful in attempting to compromise the system, because the copied memory will not preserve the address of the stored parameter. Without the address of the parameter, it is not communicated to a lockbox or to the central authority as expected and verification fails.

10           As described in the commonly-owned applications, the communications between the lockbox and the key may occur wirelessly, e.g., by infrared, radio frequency or other suitable wireless transmission. In the case of infrared transmissions, the key has an infrared transceiver and the lockbox has an infrared receiver (and possibly an infrared transmitter). The keypad and the key box of the system 10 may be similarly equipped.

15           In implementing the approach of the commonly owned applications for the system 10, several straightforward modifications are made: (1) unlike the real estate context in which a user may receive authorization for a number of days, many of the users of the system 10 are authorized for only a portion of a day; (2) unlike the real estate user who retains possession of his key and continues to use it through a number of renewals, a user in  
20           the system 10 is able to use any available standard key pad and assign his profile to the key pad in use; and (3) unlike the real estate context, update codes for special reauthorization of access privileges may only be required in the system 10 for specific situations, e.g., update codes provided by telephone authorization in the event of a power failure.

            Depending upon the particular implementation, the system 10 can include both  
25           enhanced key pads and standard key pads.

#### *Additional System Features*

            Fig. 26 is a schematic representation of a system 10', which is similar to the system 10 of Fig. 1, except several features have been added or depicted differently. In the system 10', the central computer 21' under the dealership's control is shown to represent a

network of linked computers. This network likely includes at least one computer located at the physical site where key pads are issued.

There can be a database 29, which is in addition to or instead of the database 27, for storing system information, including, e.g., inventory information such as VIN information.

5 Such VIN information may be provided by a third party to the dealership, e.g., via a link between the database 29 and the central computer network 21', such as by e-mail communication, a connection through the internet, a direct modem connection or through a network connection to the database.

There can also be a link from the central computer network 21' to an initialization  
10 function 31, which is referred to here as a Manufacturing Control System (MCS). The initialization function 31, which would typically be administered by the manufacturer, provides for initialization of system components, such as key boxes 14, including establishing settings and identifiers (e.g., serial numbers). Some of this information is communicated to the purchaser, i.e., a dealership, such as via an encrypted e-mail message, a  
15 connection through the internet, a direct connection via a modem, or through a network connection. Such communication may typically take place when components are purchased, as well as at other times, such as, e.g., following service of components. The initialization function 31 also retains this information for possible future use in repair, troubleshooting and replacement of components.

20 Fig. 26 shows the link 33 to represent that an administrator (or, in some cases, a user) can establish a telephone communication with the support function 28 and obtain update codes to authorize one or more key pads during periods where normal authorization via the dealership computer network 21 and the programming base 22 is not available, such as during a power outage or computer system failure. In this way, a dealer may be able to  
25 obtain authorization to allow key pads to be used to provide continued access to vehicles.

### *Conclusion*

The above implementations refer to the secure and remote storage of keys, and particularly, vehicle keys. It is of course expected that the same concepts could be used to manage other types of assets.

Having illustrated and described the principles of our invention with reference to several exemplary embodiments, it should be apparent to those of ordinary skill in the art that the invention may be modified in arrangement and detail without departing from such principles. We claim all such modifications that fall within the scope of the following

5 claims.